REMARKS

Initially, in the Office Action dated December 13, 2004, claims 24-30 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2002/0133793 A1 (Ginter et al.).

By the present response, Applicants have amended claims 24-30 to further clarify the invention. Claims 24-30 remain pending in the present application.

35 U.S.C. §102 Rejections

Claims 24-30 have been rejected under 35 U.S.C. §102(e) as being anticipated by Ginter et al. Applicants respectfully traverse these rejections.

Ginter et al. discloses systems and method for secure transaction management and electronic rights protection. Electronic appliances such as computers help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure change of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions.

Regarding claims 24, 26 and 28, Applicants submit that Ginter et al. does not disclose or suggest the limitations in the combination of each of these claims of, inter alia, receiving a form at a designated worker from a network in which the form

contains terms relevant to different workers encrypted by using different encrypting keys corresponding to the different workers, or decrypting an encrypted form of the form received at the designated worker from the network by using a decrypting key corresponding to the designated worker, or encrypting a certain term of a plurality of terms of a form relevant to a certain worker by using an encrypting key corresponding to the certain worker. Ginter et al. discloses that the security of secured database 610 files may be further proved by segmenting the records into "compartments". Different encryption/decryption keys may be used to protect different "compartments". This strategy can be used to limit the amount of information within secured database 610 that is encrypted with a single key. Another technique for increasing security of secured database 610 may be to encrypt different portions of the same records with different keys so that more than one key may be needed to decrypt those records. (See Fig. 32 and paragraph 1355.) In other words, Ginter et al. is directed to a transaction management with a high level of security for VDE processes in information storage and communication, establishing security at each node (see paragraph [0023] and abstract). In contrast, the limitations in the claims of the present application are related to providing a workflow system in which respective workers who check and process a plurality of divided data blocks within a document are inhibited from monitoring their checked/processed data blocks with each other (see page 3, lines 19-23). Ginter et al. does not disclose or suggest receiving a form at a designated worker from a network in which the form contains terms relevant to different workers encrypted by using different encrypting

keys corresponding to the different workers, or decrypting an encrypted term of the form received at the designated worker from the network by using a decryption key corresponding to the designated worker.

The Examiner asserts that the limitations in the claims of the present application are disclosed in Ginter et al. at paragraphs [0184], [0211], [0533], [1355], [1723], [1840], [2121], and claim 30. The Examiner fails to associate each of these paragraphs to each specific limitation in the claims of the present application. However, these paragraphs merely disclose: a simultaneous pre-defined increment type that securely stores at a user site potentially highly-detailed information reflective of a user's usage of a variety of different content segment types; that the contents control information is allowed to preserve a VDE control over one or more portions of extracted content after various forms of usage of the portions; that a masked ROM 532a may cost less than flash and/or EEPROM 532b, and can be used to store permanent portions of SBU software/firmware; that the security of secure database 610 files may be further improved by segmenting the records into compartments and that different encryption/decryption keys may be used to protect different compartments; and when encrypted or otherwise secured information is delivered into a user secure VDE processing area, a portion of this information can be used as a "tag" that is first decrypted or otherwise unsecured and then compared to an expected value to confirm that the information represents expected information; that portable appliance 2600 RAM 534 may contain, for example, information which can be used to uniquely identify each instance of the portable appliance, and that

this information may be employed in authentication, verification, decryption, and/or encryption processes; and that audit information that is destined for different auditors may be encrypted by different one or more encryption keys which have been securely provided by each auditors VDE node and communicated for inclusion in a user's permission record (S) as a required step, for example, during object registration and that this provides additional security to further ensure that an auditor may only access information to which he is authorized. This is not receiving a form at a designated worker from a network in which the form contains terms relevant to different workers encrypted by using different encrypting keys corresponding to the different workers, as recited in the claims of the present application. Ginter et al. does not disclose or suggest forms containing terms relevant to different workers. Further, these portions of Ginter et al. do not disclose or suggest decrypting an encrypted term of the form received by using a decrypting key corresponding to the designated worker, or encrypting a certain term of a plurality of terms of a form relevant to a certain worker by using an encrypting key corresponding to the certain worker. Ginter et al. merely relates to providing a distributed virtual distribution environment (VDE) that enforces a secure chain of handling and control use of electronically stored or disseminated information. Ginter et al. does not disclose or suggest a term of a plurality of terms of the form being encrypted or decrypted, or the certain term encrypted or decrypted using keys corresponding to certain workers, as recited in the claims of the present application.

Regarding claims 25, 27, 29 and 30, Applicants submit that these claims are dependent on one of independent claims 24, 26 and 28 and, therefore, are patentable at least for the same reasons noted previously regarding these independent claims. For example, Applicants submit that Ginter et al. does not disclose or suggest whether each of the terms included in the form is decrypted and whether the term which cannot be decrypted is to be displayed, or displaying a column of a term which cannot be decrypted in a format of a blank, when the encrypted term of the form is decrypted by using an another decrypting key corresponding to the another work.

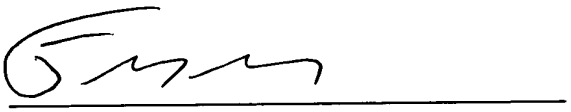
Accordingly, Applicants submit that Ginter et al. does not disclose or suggest the limitations in the combination of each of claims 24-30 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 24-30 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger & Malur, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. 500.36734CX1).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 684-1120